

IN THE CLAIMS

1. (currently amended) In a distributed network having a number of server computers and associated client devices, method of enforcing an anti-virus security policy, comprising:

updating a virus monitor with current rules and policies in an operating procedures and policy file received from a controller;

querying each of the client devices to determine if each of the client devices has an appropriate anti-virus software installed;

identifying those queried client devices not having the appropriate anti-virus software as target client devices;

locking all communications channels of the target client devices to a an anti-virus software installation server; ~~and~~

installing the appropriate anti-virus software to all target client devices;

when a visitor client device is connected to the network, locking all communication channels of the visitor client device to the anti-virus software installation server;

scanning the visitor client device using a virus scan server module; and

granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is free of viruses and has other anti-virus software or has the appropriate anti-virus software.

2. (cancelled)

3. (cancelled)

4. (currently amended) A method as recited in claim 1 ~~2~~, further comprising:

posting a notification that the target client devices and the ~~newly-connected~~ visitor client devices are prevented from communicating with other systems in the network until such time as the appropriate anti-virus software has been installed therein.

5. (currently amended) A method as recited in claim 1 ~~2~~, further comprising:

once the appropriate anti-virus software has been installed in the target client devices or the visitor ~~newly-connected~~ client devices,

relinquishing the lock on the communication channels for the newly connected client devices and the target client devices such that the target client devices and the visitor ~~newly-connected~~ client devices can communicate with the other devices of network.

6. (cancelled)

7. (cancelled)

8. (currently amended) A method as recited in claim 5 ~~7~~, further comprising:

periodically determining validity of the credential; and
granting a new credential only if the visitor client device has not been infected by a computer virus.

9. (original) A method as recited in claim 8, further comprising:
invalidating the credential when it is determined to not be valid.

10. (currently amended) A method as recited in claim ~~8~~ 7, wherein the
credential is not valid after a period of time as determined by the granting.

11. (currently amended) In a distributed network having a number of server computers and associated client devices, computer program product for enforcing an anti-virus security policy, comprising:

computer code for updating a virus monitor with current rules and policies in an operating procedures and policy file received from a controller;

computer code for querying each of the client devices to determine if each of the client devices has an appropriate anti-virus software installed;

computer code for identifying those queried client devices not having the appropriate anti-virus software as target client devices;

computer code for locking all communications channels of the target client devices to a an anti-virus software installation server; and

computer code for installing the appropriate anti-virus software to all target client devices;

when a visitor client device is connected to the network, computer code for locking all communication channels of the visitor client device to the anti-virus software installation server;

computer code for scanning the visitor client device using a virus scan server module; and

computer code for granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is free of viruses and has other anti-virus software or has the appropriate anti-virus software.

12. (cancelled)

13. (cancelled)

14. (currently amended) Computer program product as recited in claim 11
12, further comprising:

computer code for posting a notification that the target client devices and the ~~newly-connected~~ visitor client devices are prevented from communicating with other systems in the network until such time as the appropriate anti-virus software has been installed therein.

15. (currently amended) Computer program product as recited in claim 11
a2, further comprising:

once the appropriate anti-virus software has been installed in the target client devices or the visitor ~~newly-connected~~ client devices,

computer code for relinquishing the lock on the communication channels for the newly connected client devices and the target client devices such that the target client devices and the visitor ~~newly-connected~~ client devices can communicate with the other devices of network.

16. (cancelled)

17. (cancelled)

18. (currently amended) Computer program product as recited in claim 15
17, further comprising:

computer code for periodically determining validity of the credential; and
computer code for granting a new credential only if the visitor client device has not been infected by a computer virus.

19. (original) Computer program product as recited in claim 18, further comprising:

invalidating the credential when it is determined to not be valid.

20. (currently amended) Computer program product as recited in claim ~~18~~ 17, wherein the credential not valid after a period of time as determined by the granting.

21. (new) A method as recited in claim 1 further comprising determining whether a transmission protocol to communicate data in the network utilizes encryption and not locking all communication channels if encryption is used.